

Notice of Allowability

Application No.

09/895,057

Examiner

Ellen C. Tran

Applicant(s)

JUTZI ET AL.

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 12 July 2007 and 11 September 2007.
2. ☒ The allowed claim(s) is/are 1-5, 7-15, 17-25 and 27-30.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date 11 September 2007.
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

Ellen Tran
ELLEN TRAN
PATENT EXAMINER
ART 2134

DETAILED ACTION

1. In response to amendment filed on 12 July 2007 and Examiner Initiated Interview on 11 September 2007. Claims 6, 16, and 26 are canceled. Claims 1, 7, 11, 17, and 21 have been amended. Amendments to the claims are accepted.
2. An examiner's amendment to the record is attached. Please enter entire claim set. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. The examiner's amendment was authorized by attorney of record Rohan G. Sabapathypillai in phone interview on 21 August 2007 and confirming email sent on 30 August 2007.

Response to Arguments

- 3 Applicant's arguments filed 12 July 2007 have been fully considered and they are persuasive.

Allowable Subject Matter

4. Claims 1-5, 7-15, 17-25, and 27-30 are allowed.

Conclusion

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance".

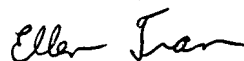
Art Unit: 2134

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is

(571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Ellen. Tran
Patent Examiner
Technology Center 2134
11 September 2007

Examiner's Amendment

This listing of the claims will replace all prior versions and listings of the claims in the application:

Listing of Claims:

1. (Currently amended) A method comprising:

performing security authentication of a content driver by a content decryption component in order to verify an identity of the content driver as a secure content driver, wherein the content driver and the content decryption component are located within a kernel application space, wherein the kernel application space is modified for registering the secure content driver with the content decryption component in order for the secure content driver to receive security identity authentication, wherein the content decryption component is tamper-resistant;

receiving an encrypted content stream from the secure content driver;

performing integrity authentication of a run-time image of the secure content driver; and

while integrity authentication of the secure content driver is verified, streaming decrypted content to the secure content driver to enable playback of the decrypted content to a user,

wherein performing integrity authentication further comprises:

decrypting the encrypted content stream received from the secure content driver;

while decrypting the received encrypted content stream, performing a hash value calculation of code segments that perform functionality of the secure content driver while loaded in memory;

selecting a stored digital signature of the run-time image of the secure content driver;

decrypting the digital signature to reveal a run-time hash value;

comparing the computed hash value with the run-time hash value of the secure content driver; and

while the calculated hash value matches the run-time hash value of the secure content driver, repeating the decryption, the performing, the selecting and the comparing until decryption of the received encrypted content stream is complete.

2. (Previously Presented) The method of claim 1, wherein performing security authentication further comprises:

locating authorization information of the secure content driver;

decrypting the authorization information received from the secure content driver; and

authenticating an identity of the secure content driver based on the decrypted

authorization information.

3. (Original) The method of claim 2, wherein authenticating the identity further comprises:

calculating a hash value of a static image of the secure content driver prior to loading the secure content driver into memory;

selecting a stored digital signature of the static image;

decrypting the stored digital signature to retrieve a pre-calculated hash value of the secure content driver;

comparing the pre-calculated hash value with the calculated hash value; and

when the calculated hash value matches the pre-calculated hash value of the secure content driver, notifying the secure content driver of successful security authentication.

4. (Original) The method of claim 1, wherein performing security authentication further comprises:

once security authentication of the content driver is established, determining a run-time at memory location of the secure content driver; and

establishing a function entry point for receiving the stream of encrypted content from the secure content driver.

5. (Original) The method of claim 1, further comprising:

receiving a content decryption key in order to enable decryption of encrypted content streams received from the secure content driver;

receiving a digital signature of a static image of the secure content driver; and

receiving a digital signature of a run-time image of the secure content driver.

6. (Cancelled).

7. (Currently Amended) A method comprising:

establishing security authentication from a content decryption component, such that a content driver is verified as a secure content driver, wherein the content driver and the content decryption component are located within a kernel application space, wherein the kernel

Art Unit: 2134

application space is modified for registering the secure content driver with the content decryption component in order for the secure content driver to receive security identity authentication, and wherein the content decryption component is tamper-resistant;

when establishment of security authentication is successful, receiving access to a callback function in order to receive clear, decrypted content streams from the content decryption component;

receiving a stream of encrypted content;

while establishing integrity authentication of a run-time image of the secure content driver, streaming the encrypted content to the content decryption component; and

when security authentication is successfully established, receiving clear, decrypted content from the content decryption component via the received callback function,

wherein establishing integrity authentication further comprises:

decrypting the encrypted content stream received from the secure content driver;

while decrypting the received encrypted content stream, performing a hash value calculation of code segments that perform functionality of the secure content driver while loaded in memory;

selecting a stored digital signature of the run-time image of the secure content driver;

decrypting the digital signature to reveal a run-time hash value;

comparing the computed hash value with the run-time hash value of the secure content driver; and

while the calculated hash value matches the run-time hash value of the secure content driver, repeating the decryption, the performing, the selecting and the comparing until decryption of the received encrypted content stream is complete.

8. (Original) The method of claim 7, wherein establishing security verification further comprises:

receiving a request for authorization information from the content decryption component;
transmitting the requested authorization information to the content decryption

component; and

when security authentication is successfully established, receiving notification of successful security authentication from the content decryption component, such that the content driver is established as the secure content driver.

9. (Original) The method of claim 7, wherein establishing security authentication further comprises:

once security authentication is established, providing content decryption component with a memory location wherein the secure content driver is loaded at run-time; and

providing the content decryption component with a function entry point for receiving the stream of encrypted content.

10. (Original) The method of claim 7, wherein receiving encrypted content further comprises:
receiving encrypted content from a content source reader; and

receiving a direction from a content driver to stream the encrypted content to the content decryption component.

11. (Currently amended) A computer readable storage medium including program instruction that directs a computer to function in a specified manner when executed by a processor, the program instructions comprising:

performing security authentication of a content driver by a content decryption component in order to verify an identity of the content driver as a secure content driver, wherein the content driver and the content decryption component are located within a kernel application space, wherein the kernel application space is modified for registering the secure content driver with the content decryption component in order for the secure content driver to receive security identity authentication, and wherein the content decryption component is tamper-resistant;

receiving an encrypted content stream from the secure content driver;

performing integrity authentication of a run-time image of the secure content driver; and

while integrity authentication of the secure content driver is verified, streaming decrypted content to the secure content driver to enable playback of the decrypted content to a user,

wherein performing integrity authentication further comprises:

decrypting the encrypted content stream received from the secure content driver;

while decrypting the received encrypted content stream, performing a hash value calculation of code segments that perform functionality of the secure content driver while loaded in memory;

selecting a stored digital signature of the run-time image of the secure content driver;

decrypting the digital signature to reveal a run-time hash value;

comparing the computed hash value with the run-time hash value of the secure content driver; and

while the calculated hash value matches the run-time hash value of the secure content driver, repeating the decryption, the performing, the selecting and the comparing until decryption of the received encrypted content stream is complete.

12. (Previously Presented) The computer readable storage medium of claim 11, wherein performing security authentication further comprises:

locating authorization information of the secure content driver;

decrypting the authorization information received from the secure content driver; and

authenticating an identity of the secure content driver based on the decrypted authorization information.

13. (Original) The computer readable storage medium of claim 12, wherein authenticating the identity further comprises:

calculating a hash value of a static image of the secure content driver prior to loading the secure content driver into memory;

selecting a stored digital signature of the static image;

decrypting the stored digital signature to retrieve a pre-calculated hash value of the secure content driver;

comparing the pre-calculated hash value with the calculated hash value; and
when the calculated hash value matches the pre-calculated hash value of the secure content driver, notifying the secure content driver of successful security authentication.

14. (Original) The computer readable storage medium of claim 11, wherein performing security authentication further comprises:

once security authentication of the content driver is established, determining a run-time at memory location of the secure content driver; and

establishing a function entry point for receiving the stream of encrypted content from the secure content driver.

15. (Original) The computer readable storage medium of claim 11, further comprising:

receiving a content decryption key in order to enable decryption of encrypted content streams received from the secure content driver;

receiving a digital signature of a static image of the secure content driver; and

receiving a digital signature of a run-time image of the secure content driver.

16. (Cancelled).

17. (Currently Amended) A computer readable storage medium including program

Art Unit: 2134

instruction that directs a computer to function in a specified manner when executed by a processor, the program instructions comprising:

establishing security authentication from a content decryption component, such that a content driver is verified as a secure content driver, wherein the content driver and the content decryption component are located within a kernel application space, wherein the kernel application space is modified for registering the secure content driver with the content decryption component in order for the secure content driver to receive security identity authentication, and wherein the content decryption component is tamper-resistant;

when establishment of security authentication is successful, receiving access to a callback function in order to receive clear, decrypted content streams from the content decryption component;

receiving a stream of encrypted content;

while establishing integrity authentication of a run-time image of the secure content driver, streaming the encrypted content to the content decryption component; and

when security authentication is successfully established, receiving clear, decrypted content from the content decryption component via the received callback function,

wherein establishing integrity authentication further comprises:

decrypting the encrypted content stream received from the secure content driver;

while decrypting the received encrypted content stream, performing a hash value calculation of code segments that perform functionality of the secure content driver while loaded in memory;

selecting a stored digital signature of the run-time image of the secure content driver;

decrypting the digital signature to reveal a run-time hash value;

comparing the computed hash value with the run-time hash value of the secure content driver; and

while the calculated hash value matches the run-time hash value of the secure content driver, repeating the decryption, the performing, the selecting and the comparing until decryption of the received encrypted content stream is complete.

18. (Original) The computer readable storage medium of claim 17, wherein establishing security verification further comprises:
receiving a request for authorization information from the content decryption component;
transmitting the requested authorization information to the content decryption component; and
when security authentication is successfully established, receiving notification of successful security authentication from the content decryption component, such that the content driver is established as the secure content driver.

19. (Original) The computer readable storage medium of claim 17, wherein establishing security authentication further comprises:
once security authentication is established, providing content decryption component with a memory location wherein the secure content driver is loaded at run-time; and

providing the content decryption component with a function entry point for receiving the stream of encrypted content.

20. (Original) The computer readable storage medium of claim 17, wherein receiving encrypted content further comprises:

receiving encrypted content from a content source reader; and

receiving a direction from a content driver to stream the encrypted content to the content decryption component.

21. (Currently Amended) An apparatus, comprising:

a processor having circuitry to execute instructions;

a content play-back interface coupled to the processor, the content play-back interface to receive encrypted content, and to enable play-back of the received encrypted content to a user; and

a storage device coupled to the processor, having sequences of instructions stored therein, which when executed by the processor cause the processor to:

perform security authentication of a content driver by a content decryption component in order to verify an identity of the content driver as a secure content driver, wherein the content driver and the content decryption component are located within a kernel application space, wherein the kernel application space is modified for registering the secure content driver with the content decryption component in order for the secure

content driver to receive security identity authentication, and wherein the content decryption component is tamper-resistant,

receive an encrypted content stream from the secure content driver,

perform integrity authentication of a run-time image of the secure content driver,

and

while integrity authentication of the secure content driver is verified, stream decrypted content to the secure content driver to enable playback of the decrypted content to a user,

wherein the instruction to perform integrity authentication further comprises the processor to:

decrypt the encrypted content stream received from the secure content driver,

while decrypting the received encrypted content stream, perform a hash value calculation of code segments that perform functionality of the secure content driver while loaded in memory,

select a stored digital signature of the run-time image of the secure content driver,

decrypt the digital signature to reveal a run-time hash value,

compare the computed hash value with the run-time hash value of the secure content driver, and

while the calculated hash value matches the run-time hash value of the secure content driver, repeat the decryption, the performing, the selecting and the

comparing until decryption of the received encrypted content stream is complete.

22. (Previously Presented) The apparatus of claim 21, wherein the instruction to perform security authentication further comprises the processor to:

locate authorization information of the secure content driver,
decrypt the authorization information received from the secure content driver, and
authenticate an identity of the secure content driver based on the decrypted authorization information.

23. (Original) The apparatus of claim 22, wherein the instruction to perform security authentication further comprises the processor to:

calculate a hash value of a static image of the secure content driver prior to loading the secure content driver into memory,
select a stored digital signature of the static image,
decrypt the digital signature to retrieve a pre-calculated hash value of the secure content driver,
compare the pre-calculated hash value with the calculated hash value, and
when the calculated hash value matches the pre-calculated hash value of the secure content driver, notify the secure content driver of successful security authentication.

24. (Original) The apparatus of claim 21, wherein the instruction to perform security authentication further comprises the processor to:

once security authentication of the content driver is established, determine a run-time at memory location of the secure content driver, and

establish a function entry point for receiving the stream of encrypted content from the secure content driver.

25. (Original) The apparatus of claim 21, wherein the processor is further caused to:
- receive a content decryption key in order to enable decryption of encrypted content streams received from the secure content driver,
 - receive a digital signature of a static image of the secure content driver, and
 - receive a digital signature of a run-time image of the secure content driver.

26. (Cancelled)

27. (Original) The apparatus of claim 21, wherein the processor is further caused to:
- establish security authentication from a content decryption component, such that a content driver is verified as a secure content driver,
 - when establishment of security authentication is successful, receive access to a callback function in order to receive clear, decrypted content streams from the content decryption component,
 - receive a stream of encrypted content,
 - stream the encrypted content to the content decryption component, and

Art Unit: 2134

when security authentication is successfully established, receive clear, decrypted content from the content decryption component via the received callback function.

28. (Original) The apparatus of claim 21, wherein the instruction to establish security verification further comprises the processor to:

receive a request for authorization information from the content decryption component,
transmit the requested authorization information to the content decryption component,
and

when security authentication is successfully established, receive notification of successful security authentication from the content decryption component, such that the content driver is established as the secure content driver.

29. (Original) The apparatus of claim 21, wherein the instruction to establish security authentication further comprises the processor to:

once security authentication is established,
provide content decryption component with a memory location wherein the secure content driver is loaded at run-time, and
provide the content decryption component with a function entry point for receiving the stream of encrypted content.

30. (Original) The apparatus of claim 21, wherein the instruction to receive encrypted content further comprises the processor to:

Art Unit: 2134

receive encrypted content from a content source reader, and
receive a direction from a content driver to stream the encrypted content to the content
decryption component.

Ellen Tran
ELLEN TRAN
PATENT EXAMINER
ART 2134